(51) International Patent Classification 7 :		(11) International Publication Number:	WO 00/67446
H04L 29/06, 29/12	**A1**	(43) International Publication Date:	9 November 2000 (09.11.00)

(54) Title: SIM BASED AUTHENTICATION MECHANISM FOR DHCRv4/v6 MESSAGES
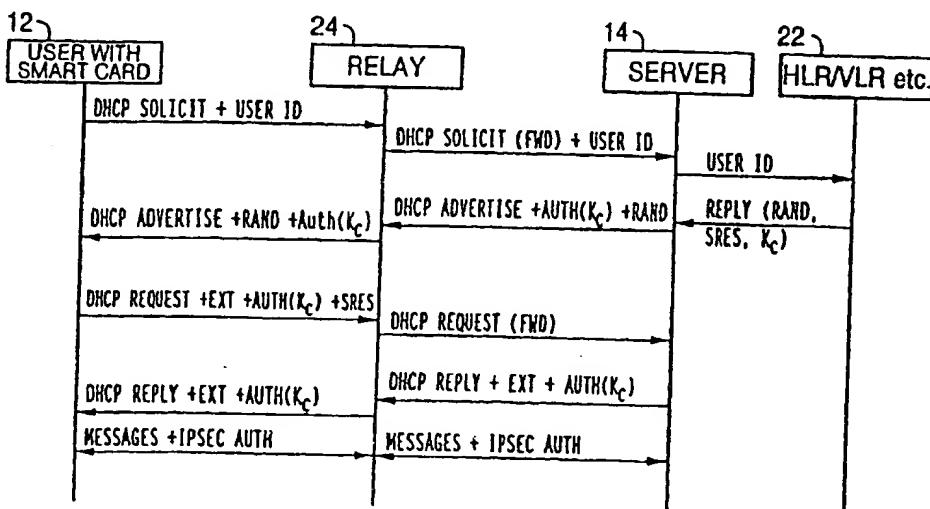
(57) Abstract

The invention is a method of providing a user (12) a terminal network address (14) in a first network (16) through which the user communicates with a data network (18) and authenticating connection of the user to the first network. The invention includes transmitting to at least one server in the first network a request to obtain the terminal network address in the first network to provide connection of the user to the data network and an identification of the user in a second network (20) through which the user communicates to the first network; transmitting the identification of the user to the second network; transmitting from the second network to the first network authentication information of the user stored in the second network associated with the identification of the user; transmitting from the first network to the user at least one advertisement of the terminal network address and information within the authentication information; and processing the received at least one advertisement and the received information within the authentication information and determining if the authentication information is correct.

SIM BASED AUTHENTICATION MECHANISM FOR DHCRv4/v6 MESSAGES

The present invention relates to methods for authenticating users (terminals in data networks) and the assignment of addresses to terminals which access data networks.

The dynamic host configuration protocol (DHCP) proposes authentication (auth) extension to guarantee that only authorized users have access to a packet data network (IP networks). The service provider network providing connectivity for a user to a packet data network has to authenticate the user (wireless terminal) during the network registration and address allocation procedure. Typically, mobile networks utilize a dynamic addressing scheme which is implemented using the DHCP protocol to connect users to network devices which connect the user to the packet data network. However, it should be understood that utilization of the DHCP protocol is not limited to wireless networks. The DHCPv4 and the DHCPv6 protocols enable dynamic configuration of IP addresses and options and use the User Data Protocol (UDP) as the communication protocol. The network entities utilized in the DHCPv4 and DHCPv6 protocols are the server, the user and an optional relay. The server is the entity that distributes network addresses and information to the users. The optional relay provides forwarding of DHCP messages so that one DHCP server serves many subnetworks instead of one server being assigned to each subnetwork. All communications between the DHCP user and the DHCP server take place utilizing a request-reply style

message exchange. All DHCP messages may also contain one or more
options (DHCPv4)/extensions (DHCPv6) that carry additional useful
parameters between the DHCP user and server.

5   The communications involved with the DHCPv4 protocol are illustrated in Fig.
1. While not illustrated, an optional relay may be used to forward DHCP
messages so that the server serves plural subnetworks. When a DHCPv4
user connects to a network and wishes to acquire an IPv4 address and other
work information, it first broadcasts a DHCP discover message to the network
10   in order to discover the presence of any DHCP server which may provide
connectivity of the user to a packet data network. The user receives a DHCP
offer message from all of the servers that received its DHCP discover
message which were configured to answer to the user. The DHCP offer
message includes the server's IP address and all other network information
15   which the server assumes the user will need. The user selects the DHCP
server whose DHCP offer message is the first one received and discards the
rest. The user informs the server whose DHCP offer message was accepted
with a DHCP request transmitted to the server to begin the user's use of the
IP address. The server acknowledges the request by sending the DHCP
20   acknowledgement to the user which then may start using the assigned IP
address.

Whenever the user wants to deallocate its IP address, it sends a DHCP
release message to the server. After the DHCP release message, the user
25   may not use the IP address any more. If the user needs to use the address
for a longer time than that was specified, the user has to try to renew the use
of the assigned IP address. This has to be done no later than when half of

the specified time allocated to the user has been used to have the address renewed. The user renews the address by sending a new DHCP request message to the DHCP server. If the server accepts the renewal of the IP address, it sends a DHCP acknowledgement containing new timer values to

5   the user. The server may also deny the renewal of the address by sending a DHCP non-acknowledgement to the user which forces the user to immediately stop using the IP address and revert to an initial state where restarting of the DHCP address acquisition process and authentication begins. If the server does not respond, the user has the option of sending all

10 of the DHCP servers a DHCP request message that includes the user's IP address. Any DHCP server that is configured to provide the IP address to the user may either renew the address by sending a DHCP acknowledgement or deny the address with a DHCP non-acknowledgement. If no replies are sent, the user stops using the IP address when the timer expires and has thereafter

15 to restart the DHCP protocol from the initial state.

The communications involved with the DHCPv6 protocol are illustrated in Fig. 2. When a user contacts the network, it will first generate a link-local IPv6 address according to the rules of stateless auto configuration as described in

20 RFC 2462 which specifications are incorporated herein by reference in their entirety. Thereafter, the user will receive a router advertisement and if the router advertisement tells the user to use stateful auto configuration, (i.e. DHCPv6), the user will send a DHCP solicit message to all DHCP agents multicast address to obtain one or more DHCP server addresses. The solicit

25 message may be forwarded by a DHCP relay to the all-DHCP-server multicast address of another network. If the user has been preconfigured with the IP address of a server or a relay and the server or relay is on the same network

link as the user, the user may skip the solicit message and select the DHCP protocol with the request message. A DHCP server receiving the solicit message will respond with DHCP advertisement message to inform the user about the server. The advertisement message contains a preference field

5   that informs how interested the server is in serving the particular user. If the user and the server are on the same link, the server replies directly to the user, otherwise, the advertised message is sent by the same DHCP relay that forwarded the solicit message to the server.

10   The user waits a predefined amount of time so that it has a chance to receive the DHCP advertisement messages from different servers. The DHCP user makes the selection between the DHCP servers based on the preference value by selecting the server that specifies the highest value of interest. If the user receives an advertisement message with the maximum preference value

15   of 255, it may select the respective server immediately and ignore any later received advertisement messages.

The user sends a DHCP address request message to the server it selected in order to request the network configuration parameters from the server. The

20   user requests these parameters by adding an extension concerning those parameters to the request message. By setting the 'C' bit field in the request message, the user may request a deallocation of its resources except those explicitly listed in the extensions. By setting the 'R' bit field, the user requests a deallocation of all of the resources it had previously required. These

25   deallocation requests are very useful when a user restarts because the user may have lost some or all of its previous state in the restarting process. The request message contains a transaction ID field which is a monotonically

increasing unsigned integer number that is used to identify the request message and combines it with the DHCP reply.

The server sends one DHCP reply message in response to every received
5   DHCP request message. The reply message carries all the important network information as message extensions which provides flexibility to information exchange. The transaction ID field is copied from the request message in order to associate the reply message with the correct request.

10   Whenever the DHCP user wants to deallocate some parameters it has received, it may do so by sending a DHCP release message directly to the server. The parameters that are to be released are listed as extensions. A release message without extension causes the server to release all the resources the user has acquired. Releasing parameters using the release
15   message is preferable to the aforementioned 'C' and 'R' bit fields in the request message which should only be used for cleaning up user parameters at start time.

Servers may notify the users that some of their parameters need to be
20   updated by sending a DHCP reconfigure message. The parameters which are present in the reconfigured messages extensions have to be reacquired by the user. In order to receive the new parameters, the user sends a new request message to the server which then responds with a reply message containing the parameters. See "Dynamic Host Configuration Protocol For
25   IPv6 (DHCPv6) Work in Progress DHCP Working Group 1998", J. Bound and C. Perkins and "Extensions for the Dynamic Host Configuration Protocol for

6

IPv6 Work in Progress 1998", by C. Perkins which publications are incorporated herein by reference in their entirety.

The GSM (Global System for Mobile Communications) telephone system uses
5   algorithms in the mobile user units and in the network servers which control authentication of the user to prevent unauthorized access to the network and to provide encryption of the transmissions between the terminal and networks. The GSM System is described in depth in the publication, "The GSM System for Mobile Communications" by Mouly and Pautet, Copyright 1992, which
10   publication is incorporated herein by reference in its entirety. Authentication in a GSM network is performed by the generation of a signed response SRES by both the user mobile and the network which is a function of a unique secret identifier Ki of the user mobile and a random number RAND. The signed response SRES is calculated in the subscriber identification module (SIM)
15   based upon Ki stored inside SIM and a random number RAND obtained from the network authentication center (AuC). Additionally, the user mobile and the network each perform encryption by generating a key Kc, which is a function of the same random number RAND and the secret identifier Ki of the mobile. The first authentication algorithm, which calculates SRES, is known as the A3
20   algorithm and the second algorithm, which computes Kc, which is computed each time a user mobile is authenticated, is known as the A8. However, each of the operations of authentication and computing of the ciphering key Kc requires the mobile to be programmed to perform the aforementioned computations and the secret algorithm stored in SIM.
25

The present invention is a method by which a user utilizes a single mechanism for the dual functions of obtaining an IP address in a data

network, which preferably is a packet data network or a wireless LAN network and authentication in the network providing connectivity to the data network. The authentication mechanism in a first embodiment utilizes a user identification stored in a second network providing connectivity between the

5   user and the first network which may be obtained from a smart card in the user terminal. Alternatively, in second and third embodiments, the authentication mechanism uses a user identification stored in the first network. The user identification in the second and third embodiments, like the first embodiment, may be obtained from a smart card in the user terminal.

10   The invention permits a wireless data network to authenticate the user using the user's telephone authentication information. The invention permits telephone networks to sell internet service provider (ISP) network access to customers and handle all billing in a telephony bill. In this situation, the ISP operator provides a gateway and the user's authentication is relayed to the

15   telephone network which is the manner in which cellular (for example, GSM) authentication is adapted to data networks. Utilization of a smart card approach which, in a preferred embodiment, uses SIM for authentication and billing, which also handles charges for packet data network access.

20   The use of the smart card permits the mapping of a telephone interface into a wireless IP network terminal and to charge wireless internet services to the telephone bill. A user entering a wireless internet office may utilize their smart card used in the telephone terminal and insert the smart card into a WLAN terminal. This permits evolution from telephone based services to WLAN

25   based wireless internet services while maintaining interworking with the telephone operator. Similarly, the use of the smart card may be integrated

8

into data network authentication with a single bill being used for both data and telephone services.

The present invention is a method of providing a user a terminal network

5   address in a first network through which the user communicates with a data network, which preferably is a packet data network such as internet/intranet core, and authenticating connection of the user to the first network. A request is transmitted to at least one server in the first network to obtain the terminal network address in the first network which provides connection of the user to

10   the data network and an identification of the user in the second network. In a first embodiment, the identification of the user is transmitted to the second network and authentication information of the user stored in the second network associated with the identification of the user is calculated using a user identification obtained from a user terminal smart card and transmitted

15   from the second network to the first network. In second and third embodiments, the identification of the user and authentication information, which is the user's profile in the second network, is stored in the first network. At least one advertisement of the terminal network address and information within the authentication information is transmitted from the first network to the

20   user. The received at least one advertisement and the received information within the authentication information is processed and a determination is made if the authentication information is correct. A request message is transmitted from the user to the first network which selects a server to provide connection of the user to the data network and which requests configuration

25   parameters of the first network, and authentication which is a function of a ciphering key and a signed response, which is a function of a secret parameter associated with a user and a random number contained in the

received authentication information. A determination is made with the first network if the signed response is correct and if the signed response is correct, a reply to the user with the configuration parameters of the first network and an acknowledgement which is a function of the ciphering key is made. After

5 the reply with the acknowledgement, which is a function of a ciphering key, communications between the user and the network are transmitted which may be authenticated with the ciphering key. In a preferred embodiment, the second network is a wireless network. The authentication information comprises a random number RAND, a signed response SRES which is a

10 function of the random number, and a secret identifier of the user and the ciphering key Kc. Each transmitted communication, after authentication is complete, may contain an IPSEC authentication header or alternatively, may be encrypted and/or authenticated by encapsulating security payload (ESP). Authentication of the user in the first network is performed before providing

15 the user with a terminal network address and typically before allowing the user access to the packet data network. When the second network stores the authentication information, a preferred storage is a register which stores information of the location of the mobile in the wireless network or using any alternative authentication encryption mechanism, e.g. radio link level security

20 functions.

The invention will now be described by way of example with reference to the accompanying drawings in which:

25 Fig. 1 is a diagram illustrating the operation of the prior art DHCPv4 protocol.

Fig. 2 is a diagram illustrating the operation of the prior art DHCPv6 protocol.

Fig. 3A illustrates a first exemplary network architecture and Fig. 3B illustrates a second exemplary network architecture in which the present invention may be practised.

5   Fig. 4 illustrates a modification of the DHCPv6 protocol in which a first embodiment of the present invention is practised.

Fig. 5 illustrates a modification of the DHCPv4 protocol in which a second embodiment of the present invention is practised.

10

Fig. 6 illustrates a modification of the DHCPv4 protocol in which a third embodiment of the present invention is practised.

Like parts and terminology are identified identically throughout the drawings.

15

Figs. 3A and 3B illustrate exemplary network architectures 10 and 10' in which the method of the invention is practised providing a user terminal 12, including a smart card, a terminal network address provided by a server 14 in a first network 16 through which the user communicates with a data network, which

20   preferably is a packet data network 18, and authenticates connection of the user to the first network.

The smart card associated with the user terminal 12, which may be of diverse designs, provides the user identification (USER ID) as described below in

25   conjunction with Figs. 4-6 and may be without limitation IMSI or NAI (Network Access Identifier) in accordance with RFC 2486. In a preferred embodiment,

the smart card may calculate SIM to provide the USER ID but the invention is not limited thereto.

An example of the user terminal 12 is a terminal which is a smart card

5   controlled mobile station having a master control unit, a user interface, a RF high frequency part, an audio low frequency part, a user interface, a power unit, a data transfer and an application module connection unit. The terminal is controlled by the master control unit with control programs stored therein. The user interface has a display, keypad and status indicators. The master

10   control unit produces various situation specific messages, operation instructions, and menu's on the display. A user enters information by the keypad, such as the terminal identification number, telephone number and select operations from the menus. The status indicators can preferably be used to indicate internal modes of operation of the terminal. The RF high

15   frequency part is part of a conventional mobile phone which is used to transmit and receive calls and messages using radio frequencies in a radio communication network such as a GSM network, e.g. through a mobile services switching center. The audio frequency part includes a microphone, a headphone and a buzzer.

20

The operation power for the terminal is supplied by a chargeable battery. A power unit monitors the charge station and charging of the battery. The power unit signals the master control unit when the charge status of the battery falls below a predetermined value.

25

A smart card is connected to a module and connector located in the terminal. The smart card provides an identification of the user (USER ID such as, but

12

not limited to, IMSI or NAI) with one form of the smart card implementation without limitation being SIM. The connection of the smart card during use provides the USER ID to the user terminal 12 for purposes of providing the USER ID during authentication as described below.

5

It should be understood that the network architectures 10 and 10' are only suggestive of diverse network architectures in which the present invention may be practised. The connectivity of the user terminal 12 is illustrated directly in the first embodiment 10 to a second network 20 having a home

10   location register/visiting/business location register 22, which is well known in cellular technology, such as the GSM system. However, the invention is not limited to wireless connectivity between the user terminal and the first network 16 with connectivity in the second architectures 10' of Fig. 3B between the user terminal 12 and the packet data network 18 being through an

15   intermediate wireless access network 19 and the first network 16 being one alternative. The first network preferably is an ISP or corporate IP network. Furthermore, the user 12 may be part of a wireless access network as illustrated in Fig. 3B. The relay 24 in the first network 16 corresponds to the relay described above regarding the prior art and is optional in the practice of

20   the present invention.

As used herein, the term "user" means any communication terminal including any associated computer, modem, etc., which communicates with the data network 18, mobile terminal, wireless IP terminal or other network connectable

25   terminal.

Fig. 4 illustrates a first embodiment of a method in accordance with the present invention which is practised with a modification of the DHCPv6 protocol. However, it should be understood that the invention is not limited thereto. The sequence of communications described as prior art in the

5   description of the DHCPv6 protocol in Fig. 2, which are common to the first embodiment, perform the same functions as in the prior art and will not be repeated herein. Furthermore, as illustrated in Fig. 4, while a preferred storage for authentication information regarding the user, which is calculated using the USER ID obtained from a user terminal smart card, is in a HLR/VLR

10 register 22, which is well known in wireless systems such as the GSM system, the authentication information of the user may alternatively be stored in the server 14. When the user authentication information is stored in the server 14, it is not necessary to transfer the user authentication information from the second network 20 to obtain connectivity to the network 18, in view of the

15 authentication information being on hand in the first network 16 at the time the address and authentication solicitation begins. When the authentication information is stored by server 14, the USER ID (e.g. IMSI or NAI) is used to locate in the server the authentication information.

20 In the operation of the first embodiment illustrated in Fig. 4, operation begins at the top left-hand corner at the user 12 and terminates at the bottom right-hand corner between which bi-directional messages plus any IPSEC authentication are transmitted between the user 12 and the server 14. The user 12 transmits a USER ID through optional relay 24 to server 14 which

25 forwards the USER ID to the HLR/VLR register 22 of the wireless network 20. The HLR/VLR register 22 uses the USER ID to generate a random number RAND, a signed response SRES, and the ciphering key Kc, which are

identified in the HLR/VLR register by the USER ID and replies by sending this information to the server 14. The RAND, SRES and Kc are identical to their use in the GSM telephone system. The invention is not limited to user authentication information being identical to that used in the GSM system. By

5   performing authentication at this time, the authentication process is completed by the first network 16 before a server 14 offers to provide a terminal network address to the user 12 and access to the packet data network 18. This sequence avoids servers 14 offering to provide a terminal network address before the user 12 is authenticated which is a more efficient use of network

10 assets. The server 14 transmits an authentication which has been calculated using the key Kc and the random number RAND via optional relay 24 to the user 12. The user 12 uses the smart card resident therein, which preferably contains a SIM identical to that used in the GSM telephone system, which processes the received RAND to produce SRES. The user 12 checks the

15 calculated SRES for authentication with the smart card and if a match is found, the assigned DHCP advertised address is validated. If the authentication information is correct, the user 12 sends a request message that contains the SRES and an authentication performed with the key Kc to the server 14 via relay 24. If the authentication of the request is correct, the

20 server 14 replies with a reply message authenticated with the key Kc. Subsequent messages between the user and the server are also authenticated using the key Kc as indicated by bi-directional "messages + IPSEC authentication", which provides additional authentication of each message. This task is performed by placing an IPSEC header in each

25 message to take advantage of the IPSEC protocol authentication. Alternatively, messages may be encrypted and/or authenticated by the ESP or by link specific functions like GSM.

The USER ID and RAND, SRES and Kc authentication information requires separate options/extensions fields where the information is contained in the DHCPv6 protocol. The smart card user identification information may, for example, be sent in platform-specific extensions. The platform-specific

5   extension is identified to carry smart card user identification information or authentication information by using a platform class identifier extension with a suitable identification value. The current version of the DHCPv6 doesn't specify particular extensions for the solicit message which requires modification of the current form of DHCPv6, as described above, to allow

10   extensions for the solicit message or, alternatively, to create a new DHCPv6 destination option. The authentication information uses the default identification extension and optionally, the default authentication algorithm defined for DHCPv6 using Kc as the shared secret. If maintaining security is of high importance, Kc may be transformed by a hash function with the hash

15   value being used instead of the key Kc in order to maintain secrecy of the key Kc. Authenticating the offer/advertised messages is useful in prohibiting malicious hosts posing as users or servers and thereby falsifying the information sent to the users and servers.

20   Fig. 5 illustrates a second embodiment of the method of the present invention modifying the DHCPv4 protocol as described above as prior art in conjunction with Fig. 1. A relay may optionally be used in Fig. 5 which performs the same function as the relay of Fig. 4. Fig. 5 is similar to Fig. 4 regarding the information which has been added to the DHCPv4 protocol which is described

25   as prior art and is not discussed further hereinafter.

16

When mapping an authentication model to DHCP message, there may not be enough messages in a single DHCP protocol round to carry all of the required signalling. What needs to be sent is the user ID, a RAND generated from the user ID, a SRES in response to the RAND and finally a message stating the outcome of the authorisation communications. The last message that states the outcome of the authorisation protocol is embedded implicitly in a DHCP acknowledgement or non-acknowledgement or message so that both the DHCP protocol and the authorization protocol are kept in synchronization with each other. The actual authentication messages passed between the user and the DHCP server have been discussed above.

A third embodiment of the invention illustrated in Fig. 6 which is a modification of the embodiment of Fig. 5, involves the transmission of authentication information using the following communications in multiple DHCP protocol rounds:

1. The user 12 sends a DHCP solicit message.

2. The DHCP server(s) 14 send DHCP advertisement messages.

3. The user 12 sends user identification information in a DHCP request message to a selected DHCP server 14.

4. The selected DHCP server 14 sends the user ID to the HLR/VLR 22 and the HLR/VLR replies with a RAND, SRES and K_c to the selected server.

5. The selected DHCP server 14 sends the RAND, SRES and K_c to the user 12 in a DHCP message.

6. The user 12 sends a new DHCP solicit message.

7. The selected DHCP server 14 sends a new DHCP advertisement message.

8. The user 12 selects the same server 14 as in step 3 above and sends SRES information in each DHCP request message to another DHCP server.

9. The DHCP server sends an DHCP reply message.

10. Messages and IPSEC authentication are sent between the user 12, servers 14 and HLR/VLR 22.

5   With the third embodiment, it is possible to send a public key, nonces, etc. in step 2 from the DHCP server to the user prior to sending the user identification in step 3. However, it also becomes more difficult, if not impossible without modifications to the protocol code, to select the same DHCP server in step 8 as in step 3. Modifying the DHCP protocol code in

10   both the user and DHCP server will increase the complexity of the DHCP protocol states. Messages, especially in steps 2, 3, 7 and 8, can get lost so that the same DHCP server cannot be contacted twice. However, steps 6 and 7 may be omitted, thereby decreasing a possibility of losing a message. These steps can be omitted for example if step 4 includes a reason for the

15   denial, which in this case could be a special "authentication failed" option or implicitly derived from the other attached options. On the other hand, only one DHCP server may be used in a subnetwork, but this has the drawback of reducing scalability.

20   The DHCP messages containing the SIM authorization messages should be authenticated with a symmetric or asymmetric key so that the DHCP server knows which SIM authorization belongs to which user in order to prevent an outsider from copying a valid SIM authentication information into the DHCP messages.

25

Unlike a DHCPv6 server, the DHCPv4 server is not able to demand a re-registration from the user. Therefore, the lifetime of the

18

authentication/authorization and the length of the DHCP lease time have to be selected in conjunction with each other. Since one outcome of the authentication is the possibility of creating new keys as well, no keys have to be distributed between the DHCP server and the user. The keys used in

5   authenticating DHCP messages need not be changed during the lease if it is assumed that the user will not be renewing its lease infinitely. However, there may be keys in use for other purposes such as authenticating each communication between the user and a security gateway. This means that a lifetime value has to be communicated between the DHCP server and the

10   user when the authentication procedure takes place. The lifetime should be selected as a multiple of the lease lifetime taking into account the values of the lease timeout timers. When the lifetime is going to end before the next re-registration, the user includes its NAI in the re-registration message which triggers the authentication procedure.

15

The use of a smart card in both embodiments permits dynamic authentication and user identity management.

The present invention facilitates products involving WLAN networks by

20   providing a WLAN terminal having a reliable, easy and flexible authentication, authorization and a billing model for ISP's and private enterprises. The use of smart cards to implement SIM adds value as a consequence of permitting an easy and secure way to distribute the necessary secret key to the users in order to calculate SIM.

25

The use of smart cards to provide SIM has a three-fold advantage. First, smart cards are tangible. Second, the same smart card may contain multiple

value added applications, in addition to SIM, such as electronic cash. Third, the smart card supports electronic signatures. The first benefit is important for corporate information technology departments and ISP's in providing the user with an inability to duplicate the user's identity. The second benefit allows

5 operators to provide users with multiple function cards which can deploy electronic cash paying for network services. Third, electronic signatures provide a method for authentication which is applicable to future wireless office applications.

10 While the invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto without departing from the spirit and scope of the invention as defined in the appended claims. It is intended that all such modifications fall within the scope of the appended claims.

CLAIMS

1.　　A method of providing a user a terminal network address in a first network through which the user communicates with a data network and authenticating connection of the user to the first network comprising:

transmitting to at least one server in the first network a request to obtain the terminal network address in the first network which provides connection of the user to the data network and an identification of the user in a second network through which the user communicates to the first network;

transmitting the identification of the user to the second network;

transmitting from the second network to the first network authentication information of the user stored in the second network associated with the identification of the user;

transmitting from the first network to the user at least one advertisement of the terminal network address and information within the authentication information; and

processing the received at least one advertisement and the received information within the authentication information and determining if the authentication information is correct.

2.　　A method in accordance with claim 1 further comprising:

transmitting a request message from the user to the first network which selects a server to provide connection of the user to the data network and which requests configuration parameters of the first network, an authentication and a signed response which is a function of a secret parameter associated with the user and a random number contained in the received authentication information.

3.   A method in accordance with claim 2 further comprising:

determining with the first network if the signed response is correct and if the

signed response is correct replying to the user with configuration parameters

5   of the first network and an acknowledgement which is a function of the

ciphering key; and wherein

the authentication transmitted to the first network is a function of a ciphering

key.

10   4.   A method in accordance with claim 3 wherein:

after the reply with the acknowledgement, which is a function of a ciphering

key, transmitting communications between the user and the network, which

are authenticated with the ciphering key.

15   5.   A method in accordance with claim 1 wherein:

the second network is a wireless network.

6.   A method in accordance with claim 1 wherein:

the authentication information comprises a random number RAND, a signed

20   response SRES, which is a function of the random number, and a secret

identifier of the user and a ciphering key Kc.

7.   A method in accordance with claim 4 wherein:

each transmitted communication contains an IPSEC authentication header.

25

8.   A method in accordance with claim 4 wherein:

each transmitted communication is encrypted and/or

authenticated with an encapsulating security payload.

9.   A method in accordance with claim 1 wherein:

authentication of the user in the first network is performed before providing the

5   user with the terminal network address.

10.   A method in accordance with claim 5 wherein:

the authentication information is stored in the wireless network in a register

which stores information of the location of a user mobile in the wireless

10   network.

11.   A method in accordance with claim 1 wherein:

the data network is a packet data network.

15   12.   A method in accordance with claim 1 wherein:

the user is in a wireless access network.

13.   A method of providing a user a terminal network address in a first

network through which the user communicates with a data network and

20   authenticating connection of the user to the first network comprising:

transmitting to at least one server in the first network a request to obtain the

terminal network address in the first network which provides connection of the

user to the packet data network and an identification of the user in a second

network through which the user communicates to the first network;

25   transmitting from the first network to the user at least one advertisement of the

terminal network address and information within authentication information

stored in the first network which is identified by the identification of the user;

23

and processing the received at least one advertisement and the received information within the authentication information and determining if the authentication information is correct.

5   14.   A method in accordance with claim 13 further comprising:
transmitting a request message from the user to the first network which selects a server to provide connection of the user to the data network and which requests configuration parameters of the first network, an authentication and a signed response which is a function of a secret
10   parameter associated with the user and a random number contained in the received authentication information.

15.   A method in accordance with claim 14 further comprising:
determining with the first network if the signed response is correct and if the
15   signed response is correct replying to the user with configuration parameters of the first network and an acknowledgement which is a function of the ciphering key; and wherein
the authentication transmitted to the first network is a function of a ciphering key.
20

16.   A method in accordance with claim 15 wherein:
after the reply with the acknowledgement, which is a function of a ciphering key, transmitting communications between the user and the network, which are authenticated with the ciphering key.
25

17.   A method in accordance with claim 13 wherein:
the second network is a wireless network.

24

18.   A method in accordance with claim 13 wherein:

the authentication information comprises a random number RAND, a signed

response SRES which is a function of the random number, and a secret

identifier of the user and a ciphering key Kc.

5

19.   A method in accordance with claim 16 wherein:

each transmitted communication contains an IPSEC authentication header.

20.   A method in accordance with claim 16 wherein:

10   each transmitted communication is encrypted and/or

authenticated with an encapsulating security payload.

21.   A method in accordance with claim 14 wherein:

the data network is a packet data network.

15

22.   A method in accordance with claim 1 wherein:

the user is in a wireless access network.

23.   A method of providing a user a terminal network address in a first

20   network through which the user communicates with a data network and

authenticating connection of the user to the first network comprising:

transmitting to at least one server in the first network a request to obtain the

terminal network address in the first network which provides connection of the

user to the packet data network;

25   transmitting from the first network to the user at least one advertisement of the

terminal network address;

25

transmitting an identifier of the user in a second network through which the user communicates to the first network to the at least one server;

transmitting to the user information within authentication information stored in the first network which is identified by the identification of the user; and

5   the user processes the received at least one advertisement and the received information within the authentication information and determines if the authentication information is correct.

24.   A system for providing a user a terminal network address, in

10   accordance with the method of claims 1 to 12.

25.   A system for providing a user a terminal network address, in accordance with the method of claims 13 to 22.

15   26.   A system for providing a user a terminal network address, in accordance with the method of claim 23.

FIG. 1
(PRIOR ART)

FIG. 2
(PRIOR ART)

FIG. 3A

FIG. 3B

USER WITH
SMART CARD

12

WIRELESS
ACCESS
NETWORK

19

RELAY
24

PACKET DATA
NETWORK

18

ISP OR
CORPORATE IP
NETWORK

SERVER
16

1 ... n

14

WIRELESS
NETWORK OR
WIRELESS CELLULAR
OPERATOR NETWORK

HLR/
VLR

20

22

10'
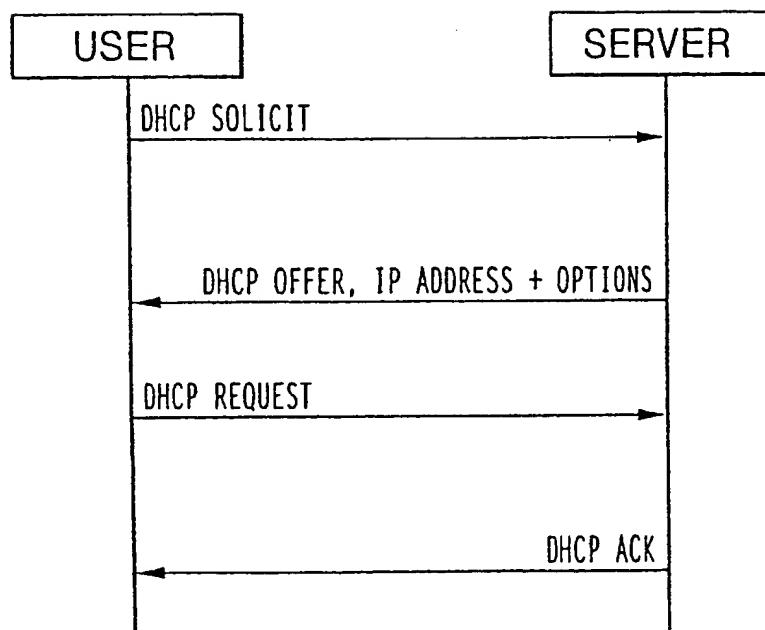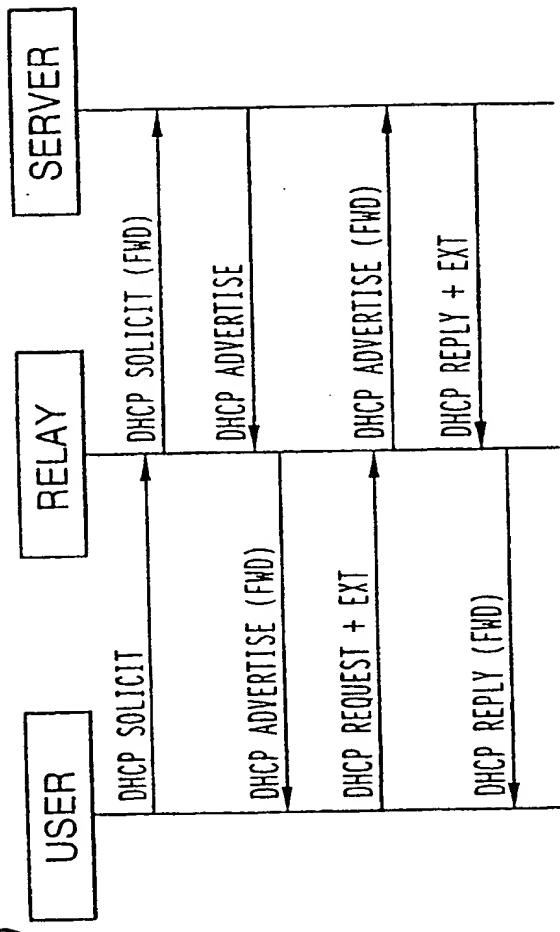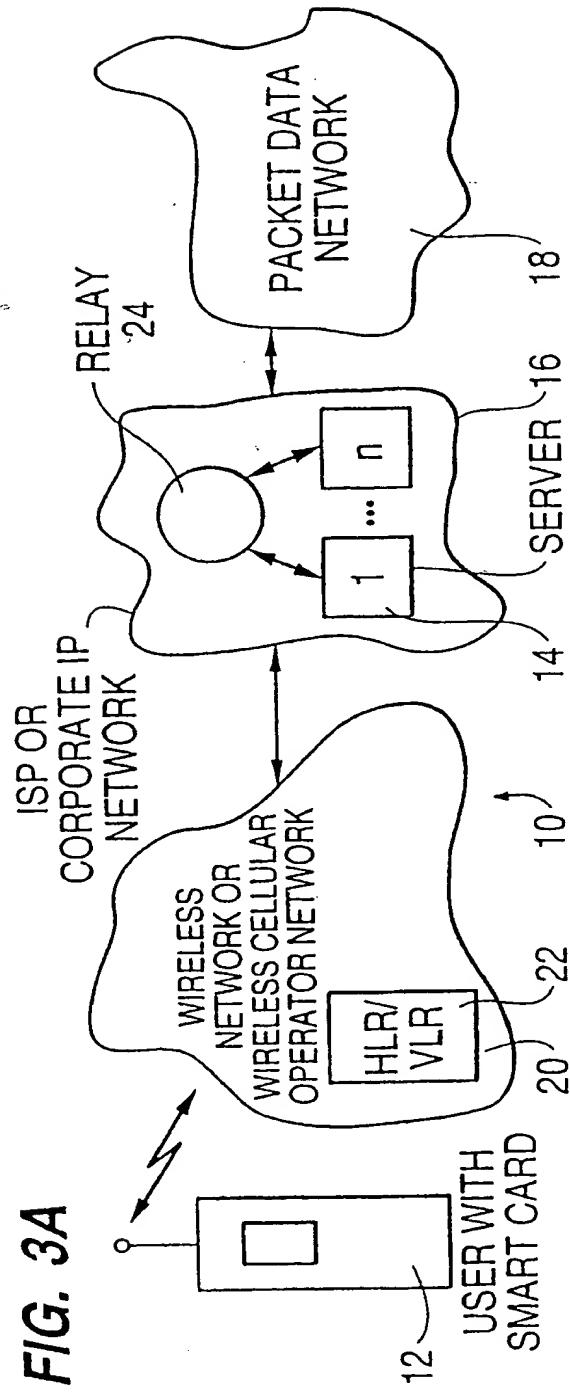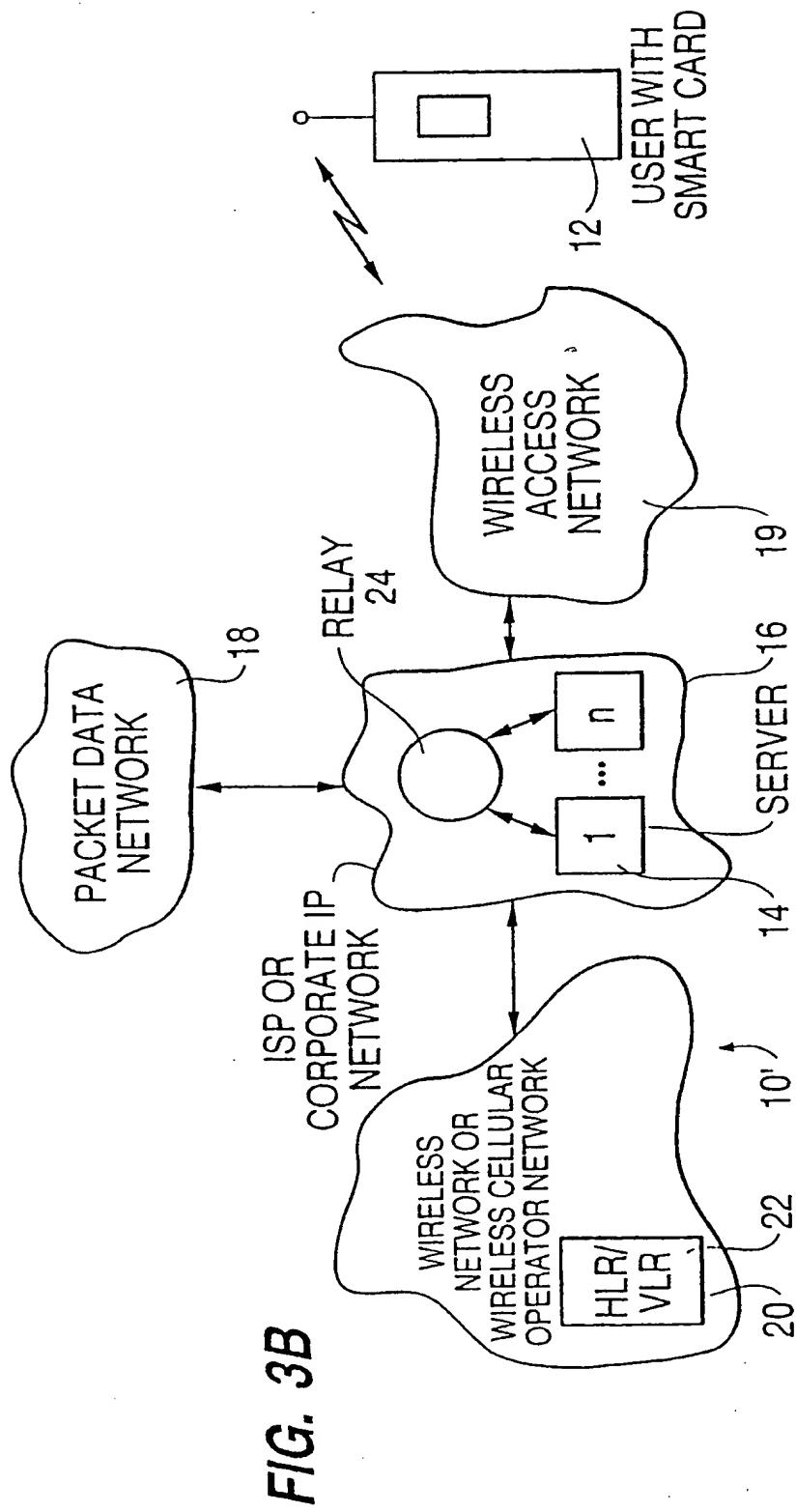
FIG. 4
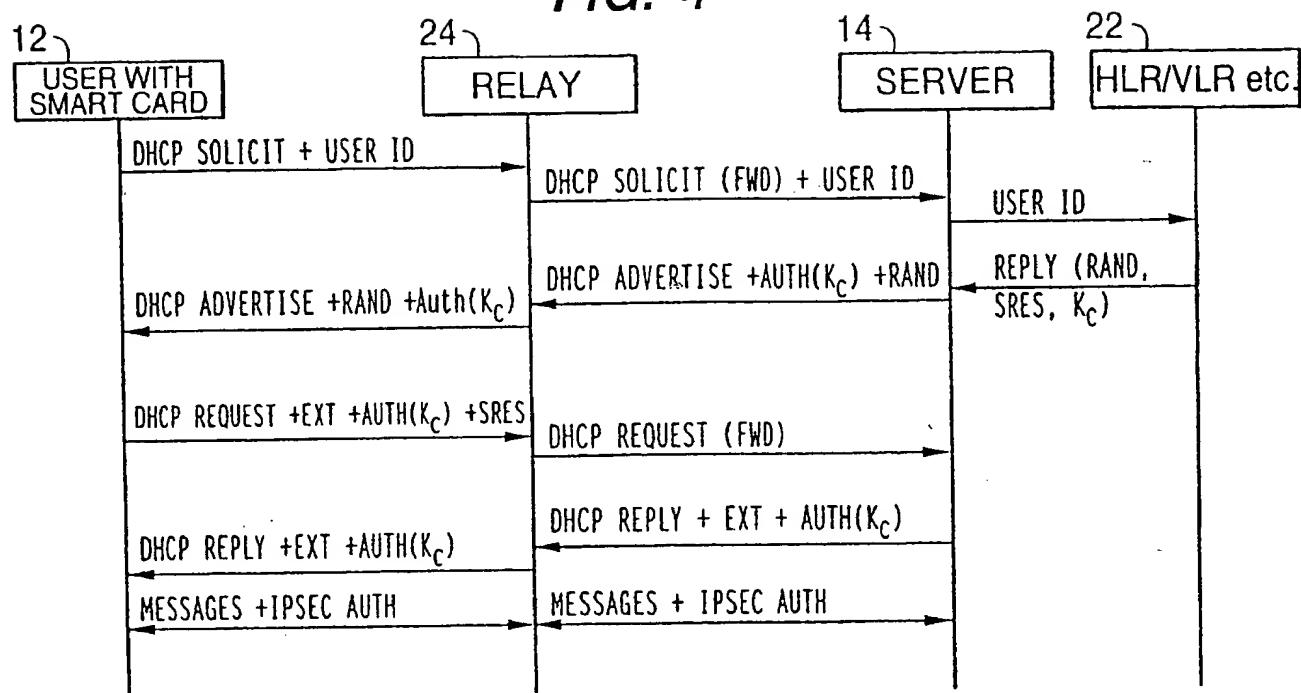
FIG. 5

FIG. 6

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04L29/06   H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document. with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOBAYASHI K ET AL: "NETWORK ACCESS CONTROL FOR DHCP ENVIRONMENT" IEICE TRANSACTIONS ON COMMUNICATIONS,JP,INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, vol. E81-B, no. 9, 1 September 1998 (1998-09-01), pages 1718-1723, XP000790192 ISSN: 0916-8516 abstract page 1719, right-hand column, line 50 -page 1721, left-hand column, line 43 --- -/--	1-26

[X] Further documents are listed in the continuation of box C.   [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2000	27/09/2000

| Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016 | Authorized officer

Adkhis, F |

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	PERKINS C E ET AL: "DHCP for mobile networking with TCP/IP" PROCEEDINGS IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, 27 June 1995 (1995-06-27), XP002132695 abstract page 260, left-hand column, line 4 -right-hand column, line 5	1-26
A	PERKINS C E ET AL: "USING DHCP WITH COMPUTERS THAT MOVE" WIRELESS NETWORKS,US,ACM, vol. 1, no. 3, 1 October 1995 (1995-10-01), pages 341-353, XP000538245 ISSN: 1022-0038 abstract page 342, left-hand column, line 21 -page 342, left-hand column, line 38	1-26